Journal of Computer Science & Its Application, December 2007, Vol. 14, No. 2

Design and Implementation of a Secure i-Voting System

***Ayo C. K, and Babajide D. O.**
Department of Computer and Information Sciences
Covenant university, PMB.1023, Ota, Ogun State, Nigeria.
{*ckayome@yahoo.com, tunjibabajide@yahoo.com,}

ABSTRACT

There is concern in many democracies about the declining rates in voter's turnout and more generally, the (perceived) trend towards political apathy. The reason is attributed to lack of trust in the political/democratic process. One of the measures considered to encourage participation in the polity is to simplify the election procedure by introducing electronic voting, and in particular, Internet voting. It is expected that this will increase voter's convenience and voter's confidence in the accuracy of election results. Internet voting means the casting of a secure and secret electronic ballot that is transmitted to electoral officials using the Internet. Internet voting is a new way of implementing democracy and eliminating some of the fallacies of paper ballot voting.

This paper proposes the development of a dynamic online voter registration system; provides a robust I-voting architecture; and designs and implements a secure Internet voting system based on Biometric features using fingerprint authentication mechanism. The system runs on platforms such as the personal computers, Operating Systems (UNIX, and Windows XP), and Browsers (Microsoft Internet Explorer, etc.). The ballots were formatted using HTML and JavaScript, and audio sound integrated into it with the use of SWiSHmax software. The server side is a java/Php application that provides access to MySQL database running on an Apache web server.

Security is incorporated into the system with the use of the N-Tier architecture incorporating the Demilitarized Zone [DMZ]. The system offers enhanced speed and efficiency, and it eliminates the "grey" area of voting, human error and bias. Further, it will allow for a broader spectrum of voters to exercise their rights anywhere there is Internet access and at the voters' convenience.

Furthermore, the system offered bimodal authentication mechanisms through the use of fingerprint and password, which helped a great deal to prevent multiple registrations of voters. It also helps to increase the confidence of voters in the electoral process. In addition, the interest of the disabled, particularly, the sight impaired is taking into consideration through the provision of audio sound to aid them in the process of casting their votes.

Keywords: Internet, e-Voting, i-Voting, ICT, Demilitarized Zone [DMZ], Security, and Biometric Authentication.

1.0 Introduction

The rapid and extensive developments of information technologies have transformed the contemporary industrialized societies into a network of societies (Global village). Information and communication technologies (ICTs) are heavily promoting and sometimes dictating changes in business, economy, culture, and the world at large. Politics and public administration are no exception to this mega trend. With the increasing penetration of the society with

information and communication technologies, their applications in public administration (e-Government) and in democratic decision making process (e-Democracy) have been a meaningful addition to conventional procedures. Unlike other social sectors, however, implementation and utilization of ICTs in the realm of politics seem to be much slow. Electronic voting is one of such issues of concern especially in the developing nations of the world. The term "electronic voting" has been used for a large variety of systems, ranging from hand-held infrared devices, kiosk systems with touch screens used in polling stations to remote voting via the Internet.

Most Nations use a variety of different voting systems. These include: ***Paper ballots:*** Voters mark boxes next to the names of candidates or issue choices, and place them in a ballot box. The ballots are counted manually. Their drawback is that counting is laborious and subject to human error [1]. ***Mechanical lever machines:*** One way to eliminate some means of ballot tampering is to eliminate document ballots. That became possible with the introduction of the lever voting machine in 1892 [2]. Voters cast ballots by pulling down levers that correspond to each candidate or issue choice. The machines prevent voting for more than one candidate [3]. ***Punch cards:*** Voters punch holes on computer readable ballot cards. Some systems use mechanical hole-punch devices for punching the holes while others provide the voter with pins to punch out the holes. The latter have been subjected to incomplete punches, resulting in more errors in reading the cards [4]. ***Optical scan devices*** and ***Direct Recording Electronic (DRE) devices:*** Special-purpose or PC-based computers are used as voting machines. Voters use touch screens or push buttons to select choices, which are stored electronically in the memory of the machine. There are no paper ballots and no paper record independent of the electronic memory. In this paper, Internet voting (i-Voting) will be of focus.

Internet voting refers to a voting procedure whereby a secure and secret vote ballot is cast and transmitted to officials via the Internet [5]. Similarly, it refers to any method of voting in a public election in which the voter's ballot is retrieved via the Internet from a county's vote-server, presented to the voter electronically on a computer screen, marked electronically by the voter, and then transmitted back to the vote-server via the Internet [6].

Over the years there had been strong interests in voting over the Internet as a way to make voting more convenient and, it is hoped, to increase participation in elections. Internet voting is seen as a logical extension of Internet applications in commerce and government. It promises to enhance speed and efficiency standards by having database updates and tallying of the votes dynamically, eliminating the grey area of voting, human errors and bias. Further, it will allow for a broader spectrum of voters to exercise their rights to vote by breaking the barrier of distance and time [7].

Internet voting is intended as a service to the electorate, so that voters might vote more conveniently. Some permit early voting, for a period of time before Election Day. Some permit home voting, workplace voting, and in general, voting from anywhere that there is an Internet-connected computer. The hope is that with added convenience and flexibility, voter participation in elections may increase. Several security issues are prevalent in the conventional voting system while some are peculiar to I-Voting. Efficient and effective security measures must be put in place to guarantee: Voter Authentication, Ballot Privacy, Ballot Integrity, Reliable Vote Transport and Storage, Prevention of Multiple Voting, Defense against Attacks on the Client, Defense against Denial of Service Attacks on Vote Servers [6].

Internet voting is no longer a novelty and is increasingly used in the private sector for casting opinions via online polls such as those offered by newspaper websites. At the political level, the adoption of this new method, for very obvious reasons, is much less straightforward given the much higher security threshold that would have to be satisfied and the need for such a reform to be legitimated, trusted and recognized by the populace and the political class as a whole. Among the most noteworthy politically binding i-Voting experiences to date, two have occurred within political parties (The Arizona primaries [8]; [9] and the Partito Radicale [10]) and another two in government held elections (The UK and Switzerland have been among the first countries to have experimented with Internet voting in a binding way. In the UK i-Voting trials were conducted for local elections and in the Canton of Geneva a referendum with the possibility of voting via the Internet were held [10].

The rest of the paper is arranged as follows: section 2 presents the statement of problem, section 3 and 4 present the objectives of research and research methodology respectively, section 5 presents

the various design models, section 6 presents the major contributions of the paper, while the conclusion of the work is presented in section 8. The screen shots of the system are shown in the appendix.

2. Statement of the Problem

Elections are at the heart of the democratic form of government, and providing sufficient security for them is very critical to the proper functioning of democracy. There have been some disagreements among experts about the seriousness of the potential security problems with i-Voting and, what is needed to enforce it. Some of the security issues at play include:

1. the ability to ensure a secure system of authentication between the client and server, to ensure that a voter's ballot is anonymous and to ensure that there is no interference with the vote [11];
2. communication infrastructure – preventing the occurrence of a Distributed Denial of Service attack;
3. registration and authentication – preventing the occurrence of multiple registration and multiple voting by the voters; and
4. ensuring the rights to vote by people with disabilities.

Additional problems may occur with the high traffic that the servers will be experiencing on a voting day. With a high traffic of votes, the server could hang, thus compromising the success of the election. Also there is "site-jacking" where the election site would have been copied and voters would be redirected to the fake site. The original voters would not be aware of this and would think they are voting correctly. This would compromise the election as well. The multiple operations and updates of data to the several databases, coupled with the dynamic updating feature, will consume many server resources [10].

3. Objectives of this Paper

The objectives of this research are as follow:

(i) investigate and review existing voting techniques;

(ii) develop a dynamic voter registration system, incorporating the use of sound (audio) to enable the disabled as well as the abled to perform their civic rights efficiently;

(iii) provide a robust architecture to handle large volume of voter's data; and

(iv) design and develop a secure i-Voting system operating on the Biometric platform using the fingerprint authentic-tion mechanism.

4. Methodology

A prototype application was developed using modern programming languages and tools to demonstrate some functionality of a secure i-Voting system. Languages used in developing the system are the HTML (Hyper Text Markup Language), Php (Hypertext Preprocessor), Java and JavaScript. The criteria applied in selecting the languages are: (a) Platform independence; (b) License freeness; and (c) Wide use. MySQL was used for creating and managing the database of voters while Apache was used for the web server.

For the biometric authentication, the Microsoft Fingerprint Reader model 1033 was used. It is called DigitalPersona fingerprint scanner. It supports plug and play and is connected to the system through the USB port. The device is for Microsoft® Windows®-based computer; Computer/ Operating System: Windows XP Home, Professional, Tablet PC, or Media Center Edition with a Pentium 233 MHz or higher processor and 128 MB of RAM; Hard Disk Space: 45 MB of available hard disk space.

Where high levels of security are necessary, the use of passwords alone is no longer a viable means of security. Passwords are easily broken using very obtainable and common password cracking programs such as Lophtcrack, NTCrack, SmartPass, and hundreds of other software floating freely on the Internet [1]. For this research a two-factor authentication was implemented i.e. the Password (PIN) and Fingerprint.

The voting site is audio sound enabled. The corresponding audio version for each page was recorded with an MP3 device and stored as an MP3 file, converted with the SWiSHmax software and saved as a shock wave flash object with the .swf file extension which enabled the file to be embedded in the HTML document as a plug-in. The site is multilingual, with the incorporation of English, Yoruba, Hausa and Igbo versions. These are the major dialects in Nigeria.

The entire application was developed running on N-tier architecture and some of the screen shots of the system are presented under the appendix.

5. System Design

5.1 Voting system requirements

Based on the tradition of elections and voting systems, a voting system, whether using paper, electronic recording or networks such as the Internet, needs to satisfy various

requirements/principles, which are summarized below [11]; [12]; [13]; [14]:

a. ***Eligibility and Authentication*** — Only authorized voters should be able to vote;
b. ***Uniqueness*** — No voter should be able to vote more than once in a particular election;
c. ***Accuracy*** — Election systems should record the votes correctly;
d. ***Integrity*** — Votes should not be modified, forged, or deleted without detection;
e. ***Reliability*** — Election systems should work robustly, without loss of any votes, even in the face of numerous failures, including failures of voting machines and total loss of Internet communication;
f. ***Flexibility*** — Election equipment should allow for a variety of ballot question formats (e.g., write-in candidates, survey questions, multiple languages); be compatible with a variety of standard platforms and technologies; and be accessible to people with disabilities;
g. ***Convenience*** — Voters should be able to cast votes quickly with less ambiguities or minimal skills;
h. ***Certifiability*** — Election systems should be testable so that election officials have confidence that they meet the necessary criteria;
i. ***Transparency*** — Voters should be able to possess a general knowledge and understanding of the voting process; and
j. ***Cost-effectiveness*** - Election systems should be affordable and efficient.

5.2 Architecture/System Design of the i-Voting System

To achieve the stated objectives of this paper, a robust i-Voting system architecture was developed based on N-tier model. The architecture is shown below:

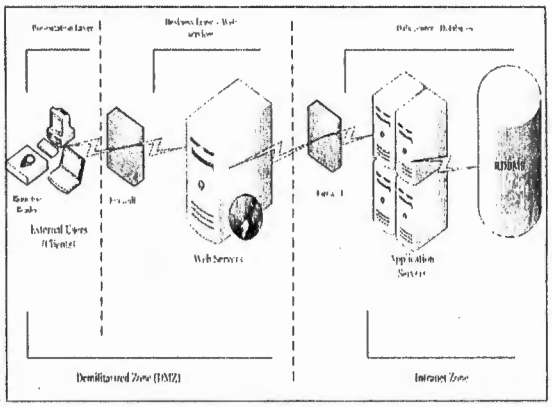


Figure 1: N-Tier Architecture (Enterprise Information System) for i-Voting

Tiers describe the division of labor of application codes on multiple machines. Tiering generally involves placing code modules on different machines in a distributed server environment. If the application code is already in layers, this makes tiering a much simpler process.

In large-scale distributed web applications, tiers are bounded by firewalls. For example, in the above architecture, a firewall is placed in front of the Presentation Tier while a second firewall is also placed in front of the Application Tier. The Presentation Tier is thus sandwiched between firewalls in what is termed the Demilitarized Zone (DMZ), while the Application and Database servers are shielded behind the second firewall in what is termed the Intranet Zone. Tiering therefore also facilitates security and allows large enterprises to shield precious internal systems from traffic originating from untrusted zones [15].

5.3 Systems Model

In modeling the above architecture, Data Flow Diagram (DFD) was used. The diagrams below were drawn using the DFD representations:

i. High-level view of the i-Voting systems functionality;
ii. Systems diagram;
iii. DFD for the i-Voting registration process;
iv. DFD for the i-Voting process;
v. DFD for the i-Voting ballot processing;

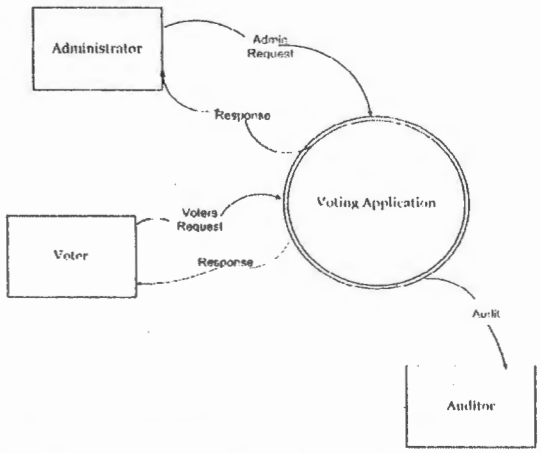


Figure 2: High-Level View of the i-Voting Systems Functionality

Presented above, is an overview of the major functional areas (voters, administrators and the auditors) of the system. This entire system is further broken down and well explained as shown below in the corresponding Data Flow Diagrams.

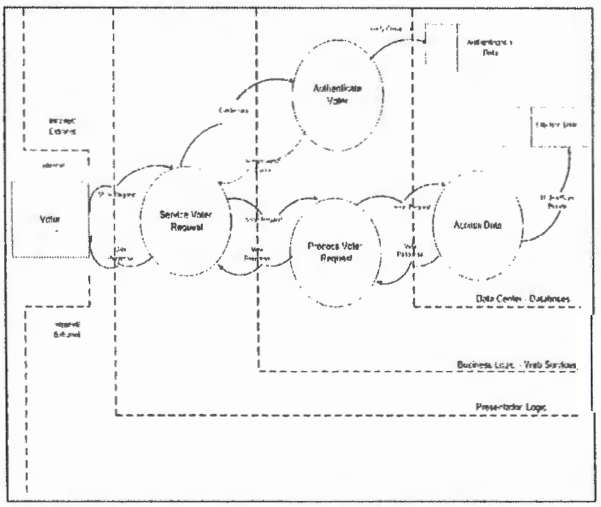


Figure 3: System Diagram for the i-Voting System

At this stage we have a better picture of the processes involved, the various data

flows and data storage for the i-Voting system

The code that interacts most closely with the user is often placed in the Presentation Tier. A second tier, which holds the application business logic and data access logic, is often referred to as the Application Tier. The third tier often houses the database or data source itself and is often referred to as the Database Tier.

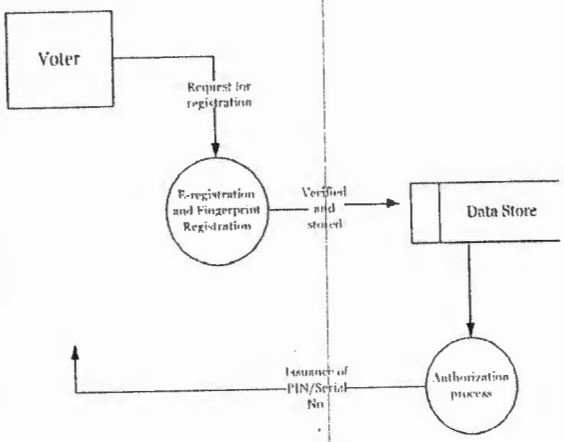


Figure 4: Data Flow Diagram for the i-Voting Registration Process

Internet voting, as described above using the DFD, proceeds in the following sequence of steps, as viewed from the perspective of a voter.

a. ***Voting preliminaries***

1. **Registration**: The potential voter must register to vote by filling the required details as required on the registration form.
2. **Fingerprint Registration**: Upon submission of the form before leaving finally, the fingerprint of each eligible voter is captured, which would be used for authentication on the actual voting day. The fingerprint image captured is mapped along side the voters particulars and the generated password. With this in place, the problem of multiple voting is eliminated.
3. **Confirmation /Authorization:** at the end of the registration process (i.e. the voter has filled the registration form and has also captured his/her fingerprint into the database); a confirmation page is sent back to the voter, which confirms the eligibility of the voter.

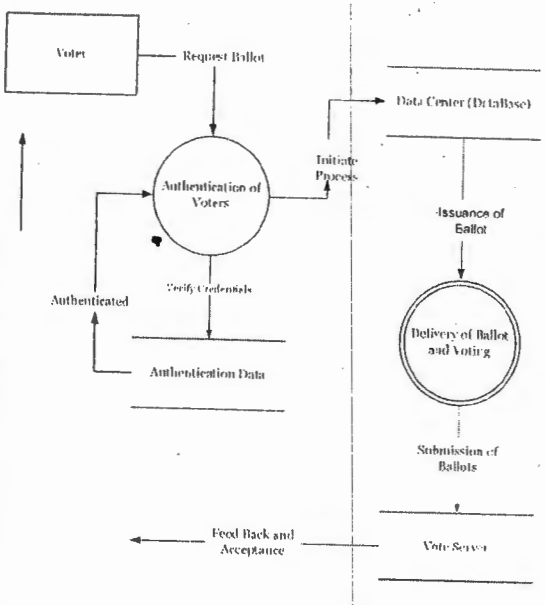


Figure 5: Data Flow Diagram for the i-Voting Process (Prevents the Occurrence of Multiple Registrations and Multiple Voting By Voters)

b. Voting:

4. **Authentication and ballot request:** when the window for i-Voting is displayed, a registered voter with authorization for Internet balloting can vote via the system. When the voter wishes to cast an Internet ballot, he visits the Internet balloting web page for the proper county and authenticates himself inputting his/her fingerprint to that server requesting a ballot in the language of his choice (note: multilingual web pages in Yoruba and Hausa [it could be increased] were also designed giving room to eligible voters who are not English literate to be able to vote).

5. **Ballot delivery:** The server will send back to the voter an image of the appropriate ballot for his or her precinct in the language requested.

6. **Voting:** The voter marks the ballot with the keyboard and or mouse (or touch-screen, if equipped).

7. **Transmission of ballot:** When the voter is finished making choices, he or she clicks a button to send the ballot (and then confirms it again). The ballot is encrypted and sent to the vote server.

8. **Acceptance and Feedback:** The vote server accepts the vote and sends feedback to the voter acknowledging that the vote has been accepted.

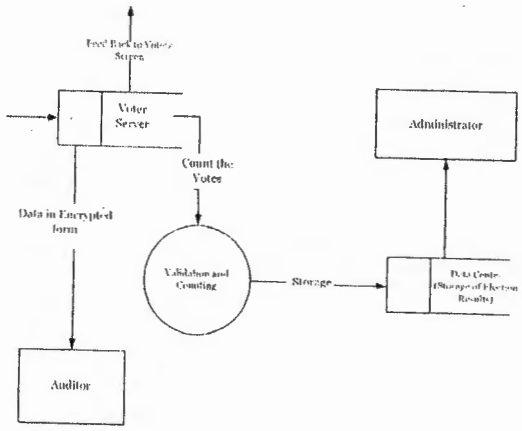


Figure 6: Data Flow Diagram for the i-Voting Ballot Processing

c. *Processing the ballot:*

9. **Validation:** The vote is validated as being from a legitimate voter who has not yet voted. It is separated permanently from the identification of the voter, and stored for counting.

10. **Audit, recount, and contest:** The votes, the separated identifications of the voters, along with other information, are retained for later audit or recount or for evidence in case the election is contested.

6. Major Contributions

Described below is a summary of the project findings/accomplishments achieved in the course of the research.

1. Registration And Authentication – preventing the occurrence of multiple registration and multiple voting by the voters:

- **Existing solutions**
  - Registration is done online generating a seven digit alphanumeric PINS.
  - Voters are asked certain questions for authentication e.g. SSN, Birth Date, etc.
  - Issuance of card with PIN numbers which would be used for authentication on the voting day.

- **Proffered Solutions**
  - For a high level of security, a two-factor authentication is used. This involves the use of a combination of authentication criteria to verify the identity of the individual. This of course is stronger than using only the PIN (One-Factor).
  - For our solution, we introduced the use of fingerprint registration during the registration process, which would also be used for authentication on the voting day. This would function along side with the generated PIN number (password) given upon registration before gaining access to the desired electronic ballot.

2. Communication Infrastructure – preventing the occurrence of a Distributed Denial of Service attack:

- **Existing solutions**
  - DDOS attacks were attempted, but system was designed to deflect these attacks
  - Intrusion Detection Software was used to filter out such attacks.
  - Internet voting was allowed only on the four days preceding the actual Election Day (March 7-11) [16].

- **Proffered solutions**
  - The use of N-tier architecture
  - The entire system is bounded by firewalls dividing the applications into the demilitarized zone and the intranet zone for effective security.

3. Ensuring the rights to vote by people with disabilities

- **Existing Solution**
  - Voting Platform for the handicapped, particularly the sight-impaired through headphones and Braille keypad [17].
- **Proffered Solution**
  - Also incorporating the use of sound (audio) devices to enable disabled as well as the abled in performing their civic rights efficiently.

8. Conclusion

Emerging technologies and the fast growing access to the Internet would eventually provide a platform for Internet voting to complement the traditional voting system which is still adopted in most countries. However, adequate security infrastructures and features such as the biometrics feature; the use of the N-Tier architecture incorporating the DMZ as well as the integration of the sound (audio) discussed in this paper must be in place to guarantee general acceptance and trust.

I-voting promises to enhance speed and efficiency standards by having database updates and tallying of the votes dynamically. It also offers the following advantages to the electoral system: cost savings associated with reduced paper handling; faster turnaround from declaration of election to close of polls; instantaneous release of elections results; and greater security and privacy over the traditional voting system.

The design of i-Voting systems would utilize modern technologies and tools such as smartcards as well as mobile voting clients. Research is therefore needed to determine to what extent such technologies are viable for voting.

References

[1.] Jan K.T. (2001): "Information Security architecture – An Integrated approach to security in the organization. CRC press LLC Pg 231 – 236.

[2.] Eric A. Fischer: "Election reform and electronic voting system (DREs): Analysis of security issues." CRS report for congress. http://www.amcham.co.nz/Newsletters/Elections20041.pdf (2003)

[3.] David Jefferson, et al: "A security analysis of the secure electronic registration and voting experiment (SERVE)" http:// www.servesecurityreport.org (2004)

[4.] California Internet Voting Task Force: "A report on the feasibility of Internet Voting". http://www.ss.ca.gov/ (2000) b.

[5.] Alexander H. Trechsel *et al*: "The European Parliament and the Challenge of Internet Voting." Policy Papers, RSC No. 03/3 http://edc.unige.ch/publications/edcreports/european_parliament_internet_voting.pdf (2003) a.

[6.] California Internet Voting Task Force: "Technical committee recommendations". http://www.ss.ca.gov/executive/ivote/ (2000) a.

[7.] Christopher L. Hixson: "Voting For the New Millennium: An Implementation of E-Voting". http://www.stetson.edu/artsci/mathcs/students/research/cs/cs498/2003/chrisH/proposal.pdf (2003)

[8.] Michael Cross: Voting against Internet elections - More delays for e-democracy as a new report raises major security concerns. http://technology.guardian.co.uk/online/story/0,3605,1145669,00.html (2004).

[9.] Wisconsin Briefs (from the Legislative Reference Bureau): "voting on the web" http://www.legis.state.wi.us/lrb/pubs/wb/00wb6.pdf (2000).

[10.] Alexander H. T., Raphael K.: "Evaluation of the use of new technologies in order to facilitate democracy in Europe - e-democratizing the parliaments and parties of Europe" http://www.utc.fr/costech/v2/_upload/fichiers/contrat/trechsel, evaluation_use_of_new_technologies.pdf (2003) b.

[11.] Eva Waskel, *et al*: "Voting system requirements" The Bell, vol. 2 No. 7 ISSN 1530-048X, http://www.thebell.net. (2000)

[12.] Liu Qi: "Security, privacy and trust considerations for e-voting". www.votoelectronico.es/.../Security,%20Privacy,%20and%20Trust%20Considerations%20for%20E-voting.pdf –

[13.] Mike B., Emmanouil M.: "Towards secure and practical e-elections in the new era". thalis.cs.unipi.gr/~emagos/overview_voting_2002.pdf (2002)

[14.] Robert K., Alexander P.: "Electronic voting: algorithm and implementation issues"http://csdl.computer.org/comp/proceedings/hicss/2003/1874/05/187450142a.pdf (2003).

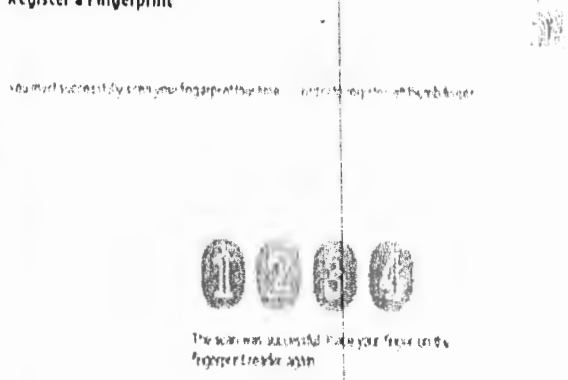
[15.] Lee V., Schneide H., Schell R. (2004): Mobile Applications: Architecture, Design, and Development, (1st print), Pearson Education, USA, pp1 – 340.

[16.] Janet Caldow: "e-Democracy: Putting Down Global Roots" http://www-1.ibm.com/industries/government/ieg/pdf/e-democracy%20putting%20down%20roots.pdf (2004).

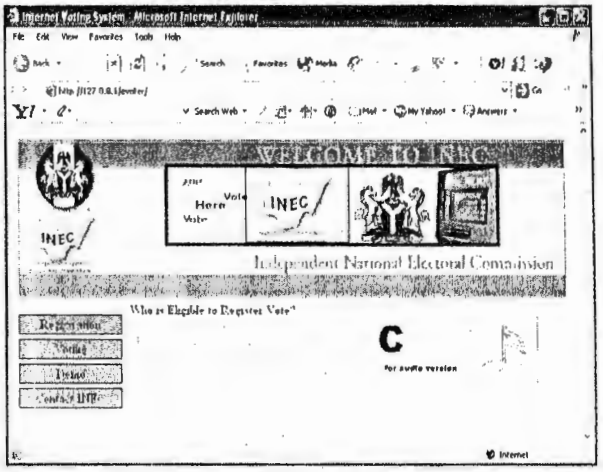
[17.] Boutin P.: Is E-voting safe? PC World,[online], http://www.pcworld.com/resource/printable/article/Φ,aid,115608,00.asp (2004).

Appendices (i) – (vi)

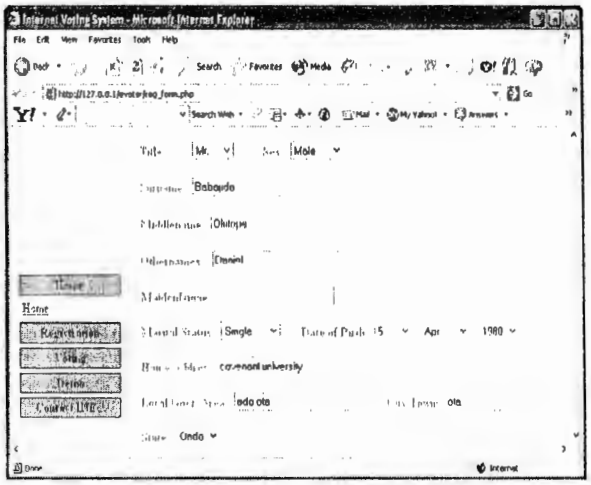
(i) Fingerprint Setup Wizard



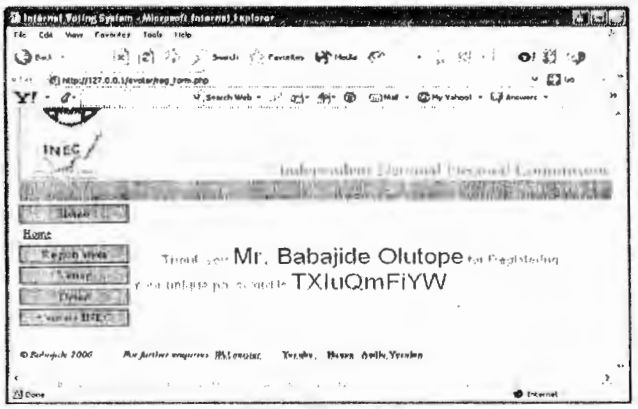
(ii) Fingerprint Capture



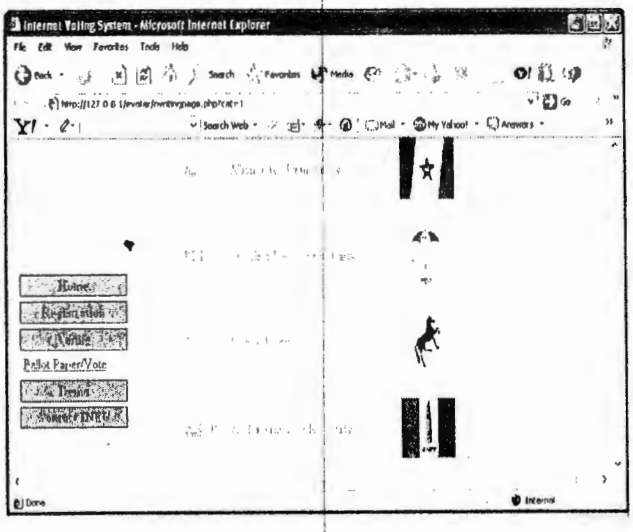
(iii) i-Voting Home Page



(iv) i-Voting Registration Form



(v) Registration Confirmation Page



(vi) Presidential Ballot Paper

Biographies of Authors

Charles K. Ayo holds a B.Sc. M.Sc. and Ph.D. in Computer Science. His research interests include: mobile computing, Internet programming, e-Business and Government, and object oriented design and development.

He is a member of the Nigerian Computer Society (NCS), and Computer Professional Registration Council of Nigeria (CPN). He is currently the Head of Computer and Information Sciences Department of Covenant University, Ota, Ogun state, Nigeria, Africa. Dr. Ayo is a member of a number of international research bodies such as the Centre for Business Information, Organization and Process Management (BIOPoM), University of Westminister; the Review Committee of the European Conference on E-Government; and the Editorial Board, Journal of Information and communication Technology for Human Development among others.

Babajide Daniel O. has his first degree (B.Sc.) in Computer Science from the University of Benin, Nigeria, M.Sc. Management Information System, Covenant University, Nigeria.

Presently, he is a Graduate Assistant with the Department of Computer and Information Sciences, Covenant University, Nigeria. He is a Cisco Certified Network Associates (CCNA) with research interests in Networking, Mobile Computing, Web Applications, E/M-Commerce and Business. He is a member of the Nigerian Computer Society (NCS), and Computer Professional Registration Council of Nigeria (CPN). Babajide D. O is currently in the employment of First Bank PLC Ibadan branch.